REMARKS

Claims 1-28 are pending in the application. Claims 1-28 were rejected under 35 U.S.C. § 103 (a).

Rejections Under 35 U.S.C. § 103 (a)

Rejection Under Karaoguz, Epstein and Inoue

Claims 1-6, 8-18 and 20-28 were rejected under 35 U.S.C. § 103 (a) as being unpatentable over U. S. Patent Application Number 2004/0059914 issued to Karaoguz dated March 25, 2004 in view of U. S. Patent Number 5,517,567 issued to Epstein on May 14, 1996, and further in view of U. S. Patent Number 6,166,649 issued to Inoue on December 26, 2000.

Applicants respectfully traverse this ground of rejection for the following reasons. First, applicants' claim 1 recites,

> "wherein one or more private keys employable for encryption and/or decryption of information are erased via an automatic cutoff of power initiated internal to the authentication device upon an attempt to move the authentication device."

As stated in the Final Office Action, the Examiner agrees that Karaoguz and Epstein do **not** teach or suggest "one or more private keys employable for encryption and/or decryption of information are erased via an automatic cutoff of power initiated internal to the authentication device". Moreover applicants note that Inoue does **not** teach or suggest the limitation either. This is because Inoue discloses that power supply to the internal power source 8 is cutoff when the signal processing means 4 detects an overvoltage. See column 3, lines 48-51. This is clearly different from applicants' claim 1 which recites "automatic cutoff of power initiated internal to the authentication device upon an attempt to move the authentication device". Thus, Inoue, similar to Karaoguz and Epstein, is missing "wherein one or more private keys employable for encryption and/or decryption of information are erased via an automatic cutoff of power initiated internal to the authentication device upon an attempt to move the authentication device", as recited in applicants' claim 1.

Second, the Examiner has cited Inoue for allegedly disclosing "cutoff of power initiated internal to the authentication device. The Final Office Action suggests that there is a motivation to combine Inoue with Karaoguz and Epstein—namely, to supply a device with improved reliability and safety by having a function which informs a user when there is an erroneous connection or abnormal power source voltage. However, applicants respectfully submit that the teachings in Karaoguz and Epstein provide no basis to conclude that a person of ordinary skill in the art would use Inoue's technique to facilitate Karaoguz's and Epstein's arrangements to arrive at the subject matter of applicants' claim 1, so the combination is improper.

Specifically, each reference addresses a problem so different from the one addressed by the other references that the respective teachings provide no motivation for the person of ordinary skill to combine them.

More specifically, Karaoguz addresses the problem of how to authenticate a user of a wireless device in a wireless network. In Karaoguz, the problem is addressed by receiving a request message from a sender to access a resource provided through a wireless network; determining first signal-generated location information of the sender; identifying the sender using the first signal-generated location information; confirming an identity of the sender; and authorizing access for the sender to access the resource.

Epstein addresses the problem of providing an improved encryption system that will prevent cellular phone fraud by authenticating the identity of the remote unit. In Epstein, the problem is addressed by (a) storing first and second secret numbers in the master and remote units; (b) generating a random number and storing the random number in the master unit; (c) combining the random number with the first secret number to produce a first intermediate number in the master unit; (d) combining the first intermediate number with the second secret number to produce a second intermediate number in the master unit; (e) combining the second intermediate number with the communications key to produce a transmission number in the master unit; (f) transmitting the transmission number and the random number from the master unit to the remote unit; (g) receiving the transmission number and the random number in the remote unit; (h) combining the random number with the first secret number to recreate the first intermediate number in the remote unit; (i) combining the first intermediate

number with the second secret number to produce the second intermediate number in the remote unit; and (j) combining the second intermediate number with the transmission number to produce the communications key in the remote unit.

Rather than addressing problems that involve authenticating a user of a wireless device in a wireless network as done by Karaoguz, or providing an improved encryption system that will prevent cellular phone fraud by authenticating the identity of the remote unit as done by Epstein, it appears that the problem being addressed by Inoue is how to inform a user of abnormal voltage supplied from a power source in a Dedicated Short-Range Communication (DSRC) on-vehicle device used in a road transportation system, e.g., electronic toll collection. In Inoue, the problem is addressed by arithmetic processing means for processing communications traffic between the DSRC on-vehicle device and an on-road unit; power supply means for receiving power supplied from a power source of a vehicle; voltage regulation means for regulating a power source voltage to supply the power source voltage supplied through the power supply means to the arithmetic processing means; abnormal voltage detection means for detecting the power source voltage supplied through the power supply means to determine whether the power source voltage is set within a predetermined range; abnormality signaling means for informing a user that the power source voltage supplied through the power supply means is abnormal; and signal processing means for driving the abnormality signaling means on the basis of an abnormal voltage signal transmitted from the abnormal voltage detection means.

In essence, Karaoguz's and Epstein's techniques are related to authentication in wireless networks, while Inoue's technique is associated with abnormal voltage supplied from a power sources.

Also, each reference discloses communication networks so different from the one disclosed by the other references that the respective teachings provide no motivation for the person of ordinary skill to combine them. Karaoguz discloses a wireless communication network environment such as IEEE 802.11, BLUETOOTH™, Ultra-Wideband (UWB), as stated in paragraph 0003. Epstein discloses communication channels such as telephone lines, satellite links, wireless networks, and cellular phone systems as stated in column 1, lines 13-18. By contrast, Inoue discloses short range

communications for Intelligent Transport Systems for traffic between a DSRC on-vehicle device and an on-road unit, as stated in column 5, lines 31-35.

Furthermore, communications in Karaoguz and Epstein does **not** appear to have distance limitations, while communications in Inoue is distance limited, i.e., short-range.

Further still, communications in Karaoguz and Epstein does **not** appear to be location dependent, while communications in Inoue is limited to a road transportation system, e.g., electronic toll collection. See column 1, lines 13-16.

Accordingly, one of ordinary skill in the art would **not** be motivated to combine a solution that provides 1) authentication of wireless devices in a wireless network or 2) an encryption system that will prevent cellular phone fraud, with 3) a system to inform a user of abnormal voltage supplied from a power source in a vehicle.

Furthermore, Karaoguz makes no mention of a system to inform a user of abnormal voltage supplied from a power source in a vehicle, nor is there a teaching in Karaoguz to suggest that there would be an improvement in Karaoguz's technique of authentication of wireless devices with Inoue's system to inform a user of abnormal voltage supplied from a power source in a vehicle. Since the teachings of Karaoguz adequately address the problem of how to authenticate a user of a wireless device in a wireless network, there is no motivation to combine with Inoue's teachings. Given that Karaoguz's technique does **not** suffer from the problems that Inoue addresses, one of ordinary skill in the art would **not** be led to try to improve Karaoguz's technique with Inoue's teachings.

Thus, one of ordinary skill in the art would **not** be motivated to modify Karaoguz and Epstein with Inoue's teachings. Consequently, applicants respectfully submit that the Examiner is relying on the use of impermissible hindsight in an attempt to reconstruct applicants' teachings by combining Karaoguz and Epstein with Inoue. Accordingly, applicants submit that the combination and resultant rejection are improper.

Therefore the proposed combination of Karaoguz and Epstein with Inoue does **not** teach or suggest all of the limitations in applicants' claim 1, and therefore claim 1 is allowable over the proposed combination. Since claims 2-13 and 23-28 depend from allowable claim 1, these claims are also allowable over the proposed combination.

Independent claims 14 and 22 each have a limitation similar to that of independent claim 1, which was shown is **not** taught by the proposed combination of Karaoguz and Epstein with Inoue. For example, claims 14 and 22 recite, "wherein one or more private keys employable for encryption and/or decryption of information are erased via an automatic cutoff of power initiated internal to the authentication device upon an attempt to move the authentication device". The proposed combination of Karaoguz and Epstein with Inoue does **not** teach or suggest this limitation for the above-mentioned reasons. Therefore, claims 14 and 22 are likewise allowable over the proposed combination. Since claims 15-21 depend from claim 14, these dependent claims are also allowable over the proposed combination.

Rejection Under Karaoguz, Epstein, Inoue and Kobayshi

Claims 7 and 19 were rejected under 35 U.S.C. § 103 (a) as being unpatentable over Karaoguz in view of Epstein and Inoue, and further in view of JP 2003323599 issued to Kobayshi.

Applicants respectfully traverse this ground of rejection for the following reasons.

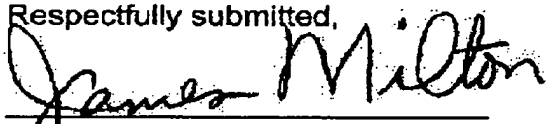
This rejection is based on the rejection under Karaoguz and Epstein with Inoue being proper. As that ground of rejection has been overcome, and none of the cited references teach or suggest "wherein one or more private keys employable for encryption and/or decryption of information are erased via an automatic cutoff of power initiated internal to the authentication device upon an attempt to move the authentication device" as recited in applicants' independent claims 1, 14 and 22, the proposed combination of Karaoguz, Epstein, Inoue and Kobayshi does **not** supply this missing element. Thus, this combination does **not** make obvious any of applicants' claims, all of which require the aforesaid limitation.

Conclusion

It is respectfully submitted that the Office Action's rejections have been overcome and that this application is now in condition for allowance. Reconsideration and allowance are, therefore, respectfully solicited.

In view of the above amendments and remarks, allowance of all claims pending is respectfully requested. If a telephone conference would be of assistance in advancing the prosecution of this application, the Examiner is invited to call applicants' attorney.

Respectfully submitted,



James Milton
Attorney for Applicants
Reg. No. 46,935

Dated: January 22, 2010

CARMEN PATTI LAW GROUP, LLC
Customer Number 47382
(312) 346-2800